一种针对 RPL 入侵检测的自适应节能算法 *

张荣槟，张　健†，唐彰国，李焕洲

(四川师范大学 网络与通信技术研究所，成都 610101)

摘　要：RPL（IPv6 routing protocol for low power and lossy networks）是 IPv6 低功耗有损无线网络的路由层协议，缺乏健全的安全保护机制且运行于资源受限的物联网设备导致容易受到网络攻击，因此在进行安全检测时应尽可能减少消耗设备资源。针对上述问题，分析了 RPL 网络的拓扑结构、RPL 的入侵检测技术和常见网络攻击的原理，论证并提出了能够降低设备功率和网络负载的自适应节能算法，最后基于 Contiki 3.0 和 Cooja 实现并验证了该算法的有效性。实验结果表明，该算法能够根据网络拓扑挑选出有效的检测节点，在保证检测率的情况下降低约 12%的设备平均功率。

关键词：路由协议；物联网；入侵检测；资源受限；自适应

中图分类号：TP393.08　　doi: 10.19734/j.issn.1001-3695.2018.07.0564

Adaptive energy-saving algorithm for RPL intrusion detection

Zhang Rongbin, Zhang Jian+, Tang Zhangguo, Li Huanzhou

(*Institute of Computer Network & Communication Technology, Sichuan Normal University, Chengdu* 610066, *China*)

Abstract: RPL (IPv6 Routing Protocol for Low power and Lossy Networks) is a routing layer protocol for IPv6 low-power lossy wireless networks. The lack of a strong security protection mechanism and running on resource-constrained IoT devices make it vulnerable to network attacks. When performing intrusion detection, it is necessary to minimize the consumption of device resources. Against the above question, this paper analyzed the network topology structure of RPL, the intrusion detection technology of RPL and the principle of common network attacks. Then, this paper expounded and proposed an adaptive energy-saving algorithm. It could reduce equipment power and network load. Finally, this paper implemented the algorithm in Contiki3 . 0, and verified the effectiveness by Cooja. Simulation experiments show that the algorithm can select effective detection nodes according to the network topology and reduce the average power of the devices by about 12% with the same true positive rate.

Key words: routing protocol; Internet of thing; intrusion detection; resource constrained; self adaptive

0　引言

物联网（Internet of things，IoT）[1]被视为继计算机和互联网之后的第三次现代信息技术革命。全球最具权威的 IT 研究与顾问咨询公司 Gartner 在预测报告[2]中指出，2021 年全球的物联网终端数量将达到 251 亿。数量有限且分布不均的 IPv4 无法支撑如此庞大的物联网络，将导致 IPv4 网络向 IPv6 转移。无线个域网是物联网网络通信的重要组成部分，包括 6LoWPAN、ZigBee、BLE 等[3]，可应用于智造工厂、智慧楼宇、智能家居等场景。6LoWPAN 相比于 ZigBee、BLE 能够支持直接接入互联网，它作为适配层通过分组和重组数据包建立 IPv6 与 IEEE802.15.4 协议之间的兼容性。低功耗和有损网络 IPv6 路由协议（RPL）[4]是由互联网工程任务组（Internet Engineering Task Force，IETF）制定的路由规范，能够满足计算能力、通信能力、能源等受限的 IoT 节点的路由要求，工作在 6LoWPAN 之上的路由层。

为了充分利用资源受限的物联网设备，通常情况下基于 RPL 的网络不会采用消耗资源较多的安全防护措施，如复杂的加密机制和基于节点的入侵检测系统（intrusion detection system，IDS）。因此，极易受到网络外部（互联网侧）和网络内部（个域网侧）的攻击。虽然加密通信可以在一定程度上抵御外部攻击，但是对于拥有可信安全密钥和凭证的内部攻击，因其可以绕过加密机制而不起作用。攻击者可利用 RPL 的安全缺陷发起的攻击行为包括：选择转发攻击（selective forwarding attacks）、陷洞攻击（sinkhole attacks）、洪泛攻击（flood attacks）、女巫攻击（sybil attacks）、DAO 不一致性攻击（DAO inconsistency attacks）等[5]。面对种类多样、手法不一的恶意攻击行为，需要构建强有力的检测技术和健全的检测架构。

1　相关研究

针对 RPL 网络的安全问题，安全研究人员开展了攻击、检测与防御的相关研究。Wallgren 等人[6]在 Contiki[7]中实现了针对 RPL 的选择转发、陷洞和克隆 ID 等攻击，并在 Cooja[8]中验证了这些攻击的破坏性。Perazzo 等人[9]在 TMote Sky 上实现了虫洞攻击，通过分析找到虫洞节点的最佳布置位置，并评估对全局丢包率和本地丢包率的影响。Pu[10]提出了一种动态阈值机制，使每个父节点基于所接收的转发错误分组的数量以及估计的正常转发错误率，动态地调整在一段时间内接受转发错误分组的阈值，以减轻 DAO 不一致性攻击。

收稿日期：2018-07-28；**修回日期：**2018-09-04　**基金项目：**四川省科技计划资助项目（2018RZ0077）

作者简介：张荣槟（1992-），男，四川雅安人，硕士研究生，主要研究方向为物联网安全；张健（1975-）（通信作者），女，四川宜宾人，副教授，博士，主要研究方向为网络安全（dctscu07@163.com）；唐彰国（1978-），男，广西桂林人，副教授，硕士，主要研究方向为网络安全；李焕洲（1974-），男，四川阆中人，教授，博士，主要研究方向为网络安全.

Alzubaidi 等人[11]提出了一个物联网 IDS,主要用于检测 6LoWPAN 内部网络中的陷洞攻击。Le 等人[12]提出基于规范的 IDS，采用分簇的思想实现混合型检测架构，支持多种攻击检测，但是要求簇头具有比普通节点更多的能量和内存资源。Medjek 等人[13]提出基于信任的分布式、多层级 IDS，在物理层构建信任平台模块，并在网络层修改 RPL 信息格式，对女巫攻击做了针对性检测，但缺乏兼容性。Raza 等人[14]首次提出针对 IoT 的 IDS——SVELTE，它是基于跳数 rank 链路质量度量的一种混合型 IDS，能够检测信息欺骗、陷洞和选择性转发攻击。Shreenivas 等人[15]扩展了 SVELTE，提出基于 ETX 链路质量度量的入侵检测算法，最后得出结论 rank 和 ETX 结合的检测率高于单独使用 rank。

通过对比分析已有针对 RPL 的入侵检测技术和系统，SVELTE 比较符合资源受限节点的安全检测思想，是一种比较高效的 IDS，然而也存在可改进之处。扩展后的 SVELTE 能够满足两种度量的安全检测，但其工作方式没有得到改善，即采用根节点定时向所有节点发送网络节点信息请求，节点依次响应并回传实时信息的方式。这种方式仍然会增加网络负载，导致通信链路利用率降低和节点能量消耗增加。针对上述 SVELTE 的不足，本文以最小化 IDS 开销为目标，提出一种自适应节能算法，该算法能够较好地适应网络拓扑变化，在保证检测率的同时降低节点能量消耗和网络负载。

2　基本概念介绍

2.1　Contiki 与 Cooja

Contiki 是 Dunkels 团队开发的事件驱动型多任务非抢占式操作系统，由 C 语言开发，通常情况下只占用 2k 字节的内存空间，非常适合资源受限的物联网设备。Contiki 包含一个小型的 IP 协议栈 uIP，完整地支持 IPv4 和 IPv6 标准，支持移植到 CC253x 系列、ARM Cortex 系列、AVR 系列等单片机硬件平台，为低功耗物联网设备接入互联网提供了有力支持。目前，Contiki 已经更新到 3.0 版本，相对 2.6 版本做了优化并且支持 IPv6 网状多播、CoAP、MQTT 等新功能。本文将基于 Contiki2.6 开发的 SVELTE 移植到 Contiki3.0，然后做进一步研究。

Cooja 是 Contiki 操作系统提供的一个网络仿真工具，支持大规模网络的开发和调试。用户通过 Cooja 可以清楚地看到节点之间的数据传递方向、网络拓扑以及节点的能量消耗状况，受到研究者的广泛使用。

2.2　RPL 协议

RPL 是专为资源受限设备设计的一种距离矢量路由协议。由 RPL 构建的网络拓扑是面向目标的有向无环图（destination oriented directed acyclic graph，DODAG），如图 1 所示。

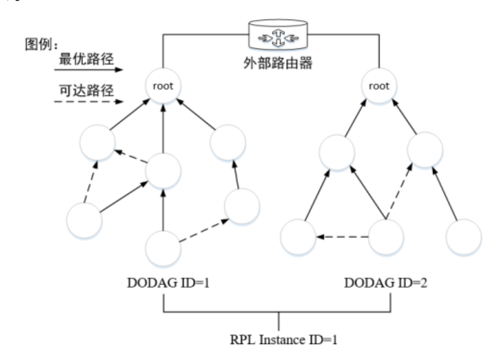


图 1　DODAG 示例

Fig. 1　DODAG example

DODAG 有一个版本号(DODAG version number)用来记录网络拓扑的版本，拓扑发生变化版本号自动加 1。多个 DODAG 可以同时属于一个 RPL 实例(RPL instance)，这些 DODAG 使用相同的 RPL 实例号(RPL instance ID)。同一个 RPL 实例中的节点只能加入到一个 DODAG 中，因此 RPL 实例号和 DODAG ID 可以确定一个 DODAG。DODAG root 是所有上行数据的目的地，也是个域网与互联网通信的 6LoWPAN 边界路由器（border router，6BR）。RPL 通过四个控制信息建立或维护网络，分别是 DODAG information solicitation（DIS）、DODAG information object（DIO）、Destination advertisement object（DAO）、Destination advertisement object acknowledgement (DAO-ACK)。具体过程如图 2 所示。

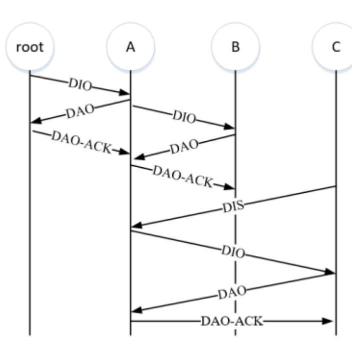


图 2　DODAG 构建过程图

Fig. 2　DODAG building process diagram

a)root 节点广播 DIO，建立上行链路；

b)root 节点附近的 A 节点侦听到来自 root 节点的 DIO，回复 DAO 信息建立下行链路，root 节点收到 A 节点的 DAO 信息后返回确认消息 DAO-ACK；

c)A 节点加入 DODAG 后也广播 DIO，通告附近的 B 节点以同样方式加入 DODAG；

d)新出现或者未收到附近广播 DIO 的 C 节点向附近的 A 节点广播 DIS，请求 DIO。

根据 RPL 规范，为了避免产生死循环，随着节点与 root 节点距离的增加 rank 必须单调增加。DODAG 中的所有节点根据统一的目标函数（objective function，OF）计算 rank,主要有两种方式，基于跳数和基于期望传输次数（expected transmission count，ETX）。ETX 指节点将数据包成功传输至目标节点所需要的重传次数，计算公式定义为

$$ETX = \frac{1}{d_r * d_f} \tag{1}$$

其中：d_r 表示成功收到应答包的概率；d_f 表示消息包被目标节点成功接收的概率。

3　自适应节能算法设计

3.1　SVELTE 的工作模式分析

文献[14]中，SVELTE 主要由 IDS-Server 和 IDS-Client 组成。IDS-Server 运行在 root 节点，包含 6LoWPAN Mapper（简称 6Mapper）、入侵检测模块和分布式迷你防火墙；IDS-Client 运行在其他节点，包含信息收集模块和中心式迷你防火墙。SVELTE 工作时，由 6Mapper 以 2 分钟的时间间隔向所有节点依次发送 mapping 请求，请求数据包大小为 5 个字节；节点收到 mapping 请求后，会将与自己相关的网络节点信息封装后返回给 6Mapper，这些信息包括该节点 IP、RPL 实例 ID、DODAG ID、DODAG 版本号、时间戳、该节点 rank、父节点 IP 以及邻居节点的 IP 和 rank，总共 13+4n

字节（每增加一个邻居节点，增加 4 个字节）；6Mapper 收到各节点返回的网络节点信息后更新本地节点信息，然后交由入侵检测模块分析。入侵检测主要是通过主观和客观（下文称为被观察节点和观察节点）信息，比较节点的 rank 值是否符合规范。

3.2　RPL 中的恶意攻击原理分析

3.2.1 陷洞攻击

恶意节点向附近节点广播 DIO 消息时，故意将其中的 rank 值减小，人为造成该节点有更好路由链路的假象，吸引附近的节点通过它路由消息。这种攻击除了会降低网络通信效率，并不一定会破坏网络正常运行。然而，当与另一种攻击结合时，它破坏性将变得非常大，如选择转发攻击。

3.2.2 选择转发攻击

作为路由节点的恶意节点根据自身意愿选择性地转发数据包，造成对路由路径的破坏。可用于过滤协议或数据导流，例如攻击者可以转发所有 RPL 控制消息而丢弃其余的消息，又如与陷洞攻击结合时可将大量的通信流量导向某一节点，形成 DoS 攻击。

3.3　自适应节能算法论证

通过分析 SVELTE 的工作模式以及恶意攻击的原理，发现只需收集部分关键节点的信息即可满足入侵检测需求。

如图 3 所示，节点 7 和 10 与其他节点只有唯一一条路径且没有子节点，称为叶子节点。叶子节点发起选择转发攻击毫无意义，因为通过自己的数据只属于自己且只能将数据发给父节点；若发起陷洞攻击，只能吸引父节点让父节点指向自己，导致父节点在网络中不可达，随即触发 SVELTE 报警。另一种节点是节点 6，它有唯一的父节点 3 和子节点 10，选择转发攻击将导致节点 10 不可达；陷洞攻击导致节点 3、6、10 脱离网络，都将触发 SVELTE 报警。所以，对于这两种节点，即使不采集节点信息，当发生攻击时也可以被发现。

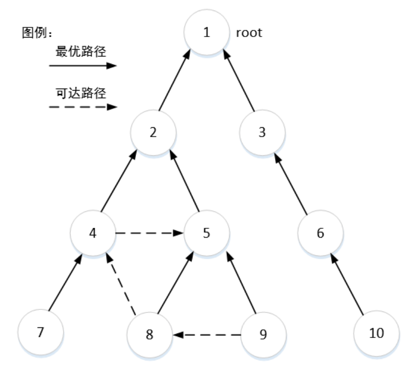


图 3　节点类型图

Fig. 3　Node type diagram

除了上述两种节点，其他节点都可能作为观察节点或被观察节点提供网络节点信息。用 $DAG(V,E)$ 来表示有向无环图，其中 V 代表网络中节点的集合，E 代表网络中邻居边的集合。本文有如下定义：

a) $P(v)$ 表示节点 v 的父节点；

b) $N(v)$ 表示节点 v 的邻居节点的集合，不包括父节点；

c) $S(v)$ 表示节点 v 的子节点的集合，有 $S(v) \subseteq N(v)$ 。

因此，叶子节点可描述为 $N(v)=0$；唯一路径中的节点描述为 $N(v)=S(v)=1$ 。

选择观察节点和被观察节点时，应首先避开以上两种节点，并遵循以下原则：

原则 1　若被观察节点 v 满足 $\{N(v)-S(v)\} \neq \varnothing$，则越大越优先考虑；

原则 2　若观察节点 v_t 满足 $v_t \in \{N(v)-S(v)\} \neq \varnothing$，且 $N(v_{t1}) > N(v_{t2})$，则 v_{t1} 优先于 v_{t2}；

原则 3　若观察节点 v_t 满足 $v_t \in \{N(v)-S(v)\} \neq \varnothing$，则 v_t 优先于 $p(v)$ 。

对于原则 1，$\{N(v)-S(v)\}$ 越大说明节点 v 成为其他节点的父节点的可能性越大，其网络位置越重要，从博弈的角度来说对该种节点的监测收益是可观的；原则 2 说明在选择观察节点时，邻居节点多的节点掌握更多的节点信息，能够对检测提供较充分的检测信息；由于 DODAG 是一种以上行数据为主的拓扑，导致父节点视野受限，原则 3 则指明在给被观察节点 v 选择观察节点 v_t 时，优先考虑节点 v 的非子邻居节点。

3.4　自适应节能算法描述

本文提出的自适应节能算法的基本思想是，当网络拓扑发生变化时首先计算节点的 $N(v)$ 和 $S(v)$ 以及它们之间的关系，然后根据原则 1 过滤叶子节点和唯一路径中的节点，最后根据原则 2 和原则 3 确定观察节点。具体描述如算法 1 所示。

算法 1　自适应节能算法

输入：网络中所有节点集合 V 。

输出：检测节点集合 V' 。

```
1 V’=Ø
2 if(DODAG_VN 未变化) then
3     exit();
4 end if;
5 for(v in V) do
6     if(v=root | N(v)=0 | N(v)=S(v)=1) then
7         continue;
8     end if;
9     if(N(v)=S(v)) then
10        添加 P(v)到 V’;
11    end if;
12    if(N(v)>S(v)) then
13        for(k in { N(v)-S(v)})do
14            if(N(k)最大) then
15                添加 n 到 V’;
16            end if;
17        end for;
18    end if;
19 end for;
20 输出 V’;
```

算法的目的是根据实际网络拓扑在满足检测信息充分的前提下，从所有节点中选择最佳的检测节点，以减少冗余节点信息的传输带来的资源消耗。

算法第 1 步初始化检测节点集合 V' 为空。算法第 2~4 步检查网络拓扑是否发生改变，若改变即引起 DODAG 版本号加 1，则执行本算法；否则退出。算法第 5~19 步按照三个原则生成检测节点集合 V' 。对于所有节点集合 V，如果节点 v 是 root 节点、叶子节点 $N(v)=0$、唯一路径中的节点 $N(v)=S(v)=1$ 中的任意之一，则跳过该节点，执行 continue，由算法 1 中的第 6-8 步表示。第 9-11 步表示，如果节点 v 的邻居节点全是子节点，即 $N(v)=S(v)$，则将父节点作为该节点的观察节点；根据原则 2，如果节点 v 存在邻居节点不是子节点，即 $N(v)>S(v)$，选邻居节点的邻居多者为该节点的观察节点，即表示为算法第 12-18 步。算法第 20 步，输出检测节点集合 V' 。

在本算法中，若网络节点集合 $V=\{v_1,v_2,\cdots,v_k,\cdots,v_n\}$ 中存在 n 个节点，其中第 k 个节点 v_k 的非子邻居数为 m（0<m<n），需要执行 $O(nm)$ 次运算。对 DODAG 版本号等的计算复杂度为 $O(1)$，因此，最多计算 $O(nm)$ 次即可得到 V'。然而，n 中的 root、叶子等节点首先应该剔除，并且通常情况下非子邻居节点的数目不会太大，所以，该算法的复杂度为 $O(nm)$，且 $O(nm)\ll O(n^2)$。

4　实验与分析

4.1　实验环境

本文实验采用的环境为惠普台式机及 Windows 10 64 位操作系统，具体配置参数如表 1 所示。

表 1　实验环境参数表

Table 1　Experimental environment parameter table

组件名	参数
CPU	Intel i5-3470 3.2GHz
RAM	4GB
VMware Workstation	14.1.1 专业版
开发平台、仿真平台	InstantContiki3.0
虚拟机内存	1GB
虚拟机处理器个数	1

面向后续对 IPv6 网状多播、CoAP、MQTT 等新功能进行进一步研究，本文所有实验及仿真基于 Contiki 3.0。本文对文献[14]中的 SVELTE 作了修改，主要有两个原因:a)本文提出的算法只需收集部分关键节点的信息，而 SVELTE 检测时的对象包括所有节点的时间戳，所以需要适当修改检测算法处理缺失节点的时间戳；b)Contiki 3.0 在部分数据结构上较 Contiki2.6 有一定改善，移植的时候需要用到新的数据结构替换。文献[15]指出，由于 Cooja 中 Tmote sky 平台资源有限，针对 ETX 的 IDS 最多支持 8 个模拟节点。本文提出的算法对节点规模较大的网络有较明显的优势，因此本文也以 8 个节点进行实验，从检测率和功率两方面作比较。

4.2　实验设置

考虑到节点分布随机性对实验的影响，本实验分为两次，每次十轮。第一次实验运行扩展后的 SVELTE，第二次实验运行扩展并加入了本算法的 SVELTE，每轮实验包含 8 个合法节点和 2 个恶意节点。所有节点组网结束后，开始采集节点信息，每五分钟记录一次节点功率，三十分钟时结束。

使用 Contiki 提供的 powertrace 模块记录每个节点工作时的 CPU、LPM、transmit、listen 电压值 (mV)，并用以下公式计算节点能耗：

$$\begin{aligned}Energy(mWs)=&\ stransimit*19.5+\\ &listen*21.8+LPM*0.0545+CPU*1.8\end{aligned}\tag{2}$$

其中:LPM 表示低功率模式，transmit 表示发送数据，listen 表示接收数据，其余数字表示各组件的工作电流 (mA)。

单个节点的时间平均功率为

$$Power(mW)=\frac{Energy(mWs)}{Time(s)}\tag{3}$$

所有节点的统计平均功率为

$$Average(Power)=\frac{\sum_{i=1}^{n}Power_i(mW)}{n}\tag{4}$$

4.3　实验结果分析

图 4 表示通过多次实验统计得出加入本文算法前后的检测率。基于对 RPL 网络特点和 SVELTE 工作模式的深入分析，发现文献[15]的检测方法存在检测信息采集冗余、资源消耗的问题。本文提出的自适应节能算法，意在过滤掉信息价值不高的节点以减少资源消耗，从图中可以看出，加入本文算法并不影响原有的检测率。本文没有修改 SVELTE 中的检测规则，仅加入了自适应节能算法，所以得到的检测率跟文献[15]相差无几，说明本文算法选择的检测节点能有效覆盖恶意节点。

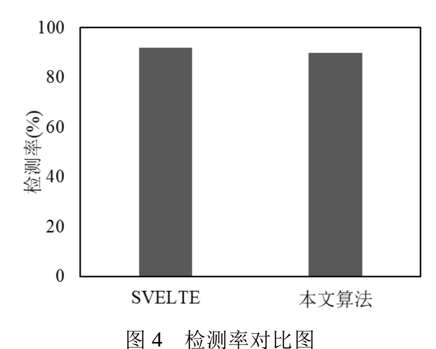


图 4　检测率对比图

Fig. 4　Comparison of detection rates

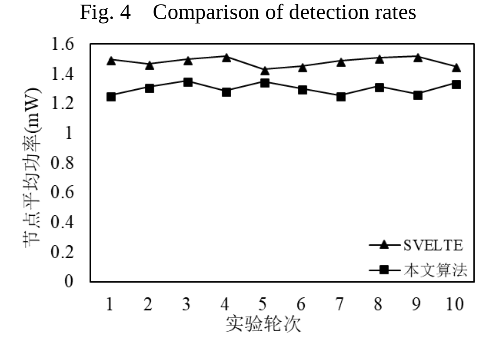


图 5　节点平均功率对比图

Fig. 5　Node average power comparison chart

图 5 表示加入本文算法前后十轮实验的节点平均功率对比折线。从图中可以看出，本文算法有效地降低了节点平均功率。计算得出，加入本文算法后总的平均功率降低了约 12%。本次实验共 10 个节点，拓扑结构导致选择的检测节点个数存在差异（约为 7~9 个），结合总平均功率的降低值分析，实验结果较合理。

5　结束语

为增强检测框架的适应能力并实现资源受限设备的有效节能，本文结合动态检测思想，主要研究了 RPL 网络入侵检测节点的选择问题。针对现有的入侵检测方法对设备资源消耗过高的问题，提出了网络拓扑自适应的节能算法，论证并验证了算法的可行性和有效性。该算法根据网络拓扑，选择有价值的检测节点，为入侵检测提供足够的检测信息。实验表明，该算法能较好地满足安全检测和节能的需求，可供借鉴于其他个域网网络技术。下一步的研究重点是将实验从资源受限且处于仿真环境中的 Tmote sky 平台迁移到真实的 CC2538 物理平台，并考虑将树莓派作为 6LoWPAN 边界路由器，解决边界路由负荷大的问题。

参考文献：

[1] Minerva R, Biru A, Rotondi D. Towards a definition of the Internet of things (IoT) [J]. IEEE Internet Initiative, 2015, 1: 1-86.

[2] Gartner. Forecast: Internet of things:endpoints and associated services, worldwide [EB/OL]. (2017) [2018-07-25]. https://www. gartner. com/doc/3840665.

[3] Al-Sarawi S, Anbar M, Alieyan K, *et al*. Internet of things (IoT)

communication protocols: review [C]//Proc of the 8th International Conference on Information Technology. 2017: 685-690.

[4] Winter T, Thubert P, Brandt A, *et al.* RPL: IPv6 routing protocol for low-power and lossy networks, RFC 6550 [R] , Fremont: Internet Engineering Task Force (IETF) , 2012.

[5] Mayzaud A, Badonnel R, Chrisment I. A taxonomy of attacks in RPL-based Internet of things [J]. International Journal of Network Security, 2016, 18(3): 459-473, .

[6] Wallgren L, Raza S, Voigt T. Routing attacks and countermeasures in the RPL-based Internet of things [J]. International Journal of Distributed Sensor Networks, 2013, 9(8): 167-174.

[7] Dunkels A, Grnvall B, Voigt T. Contiki:a lightweight and flexible operating system for tiny networked sensors [C]//Proc of IEEE International Conference on Local Computer Networks. Washington DC: IEEE Computer Society,2004: 455-462.

[8] Osterlind F, Dunkels A, Eriksson J, *et al.* Cross-level sensor network simulation with cooja [C]// Proc of the 31st IEEE Conference on Local Computer Networks. Piscataway,NJ: IEEE Press, 2006: 641-648.

[9] Perazzo P, Vallati C, Varano D, *et al*. Implementation of a wormhole attack against a rpl network: Challenges and effects [C]// Wireless On-Demand Network Systems and Services. Piscataway,NJ: IEEE Press, 2018: 95-102.

[10] Cong P. Mitigating DAO inconsistency attack in RPL-based low power and lossy networks [C]//Proc of IEEE Computing and Communication Workshop and Conference. Piscataway,NJ: IEEE Press, 2018: 570-574.

[11] Alzubaidi M, Anbar M, Al-Saleem S, *et al*. Review on mechanisms for detecting sinkhole attacks on RPLs [C]//Proc of International Conference on Information Technology. Piscataway,NJ: IEEE Press, 2017: 369-374.

[12] Le A, Loo J, Chai K K, *et al.* A specification-based IDS for detecting attacks on RPL-based network topology [J]. Information, 2016, 7(2): 25.

[13] Medjek F, Tandjaoui D, Romdhani I, *et al*. A trust-based intrusion detection system for mobile RPL based networks [C]//Proc of IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data. Piscataway,NJ: IEEE Press,2017: 735-742.

[14] Raza S, Wallgren L, Voigt T. SVELTE: real-time intrusion detection in the Internet of things [J]. Ad hoc networks, 2013, 11(8): 2661-2674.

[15] Shreenivas D, Raza S, Voigt T. Intrusion detection in the RPL-connected 6LoWPAN networks [C]// Proc of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security.New York: ACM Press, 2017: 31-38.